



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

29989 7590 06/02/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

MOORTHY, ARAVIND K

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 06/02/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/728,488 11/30/2000

Sunil K. Srivastava

50325-0108

4277

TITLE OF INVENTION: METHOD AND APPARATUS PROVIDING SECURE MULTICAST GROUP COMMUNICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$0	\$0	\$1440	09/02/2008

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

**Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

29989 7590 06/02/2008

**HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110**

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE-FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/728,488 11/30/2000 Sunil K. Srivastava 50325-0108 4277

TITLE OF INVENTION: METHOD AND APPARATUS PROVIDING SECURE MULTICAST GROUP COMMUNICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$0	\$0	\$1440	09/02/2008

EXAMINER	ART UNIT	CLASS-SUBCLASS
MOORTHY, ARAVIND K	2131	713-163000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

1

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2

3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/728,488

11/30/2000

Sunil K. Srivastava

50325-0108

4277

29989

7590

06/02/2008

EXAMINER

MOORTHY, ARAVIND K

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 06/02/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 1124 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 1124 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability**Application No.**

09/728,488

Applicant(s)

SRIVASTAVA, SUNIL K.

Examiner

Aravind K. Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERIT IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 21 February 2008.
2. ☒ The allowed claim(s) is/are 1,2,4,6,10,12,15,16,20,23,24,31,34,38,42,47,48,51,54-56,59 and 81-122.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. This is in response to the arguments filed on 21 February 2008.
2. Claims 1, 2, 4, 6, 10, 12, 15, 16, 20, 23, 24, 31, 34, 38, 42, 47, 48, 51, 54-56, 59 and 81-122 are pending in the application.
3. Claims 1, 2, 4, 6, 10, 12, 15, 16, 20, 23, 24, 31, 34, 38, 42, 47, 48, 51, 54-56, 59 and 81-122 have been allowed.
4. Claims 3, 5, 7-9, 11, 13, 14, 17-19, 21, 22, 25-30, 32, 33, 35-37, 39-41, 43-46, 49, 50, 52, 53, 57, 58 and 60-80 have been cancelled.

Allowable Subject Matter

5. Claims 1, 2, 4, 6, 10, 12, 15, 16, 20, 23, 24, 31, 34, 38, 42, 47, 48, 51, 54-56, 59 and 81-122 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards a complete, scalable approach for establishing secure multicast communication among multiple multicast proxy service nodes of domains of a replicated directory service that spans a wide area network. In one feature, the multicast proxy service nodes are arranged in a binary tree architecture at the LAN level, thereby eliminating the single point of failure of traditional approaches. In another feature, scalability is achieved by using an operationally optimized broadcast version of Diffie-Hellman key exchange that reduces the number of rounds of messages needed to exchange keys. Alternatively, scalability is achieved using a new method for coming to a shared secret in nodes of a broadcast group. Using either feature, a secured communication channel is provided among a plurality of distributed multicast proxy service nodes at the LAN level. According to another feature, a tree approach is

used to spread the multicast proxy service nodes at the WAN level, further improving scalability. A directory replication approach is used to distribute private keys of the multicast proxy service nodes, thereby achieving near perfect forward and backward security among nodes at the WAN level. The binary tree architecture is exploited to reduce the overhead involved in calculating new keys by having a local multicast key distribution node serve as a local group member and also manage joining new nodes and determining the new keys.

The closest prior art to the current application was Peyravian et al U.S. Patent No. 6,363,154 B1 (hereinafter Peyravian). Peyravian is directed towards secure messages that are sent among a group of nodes selected from a plurality of nodes that are connected to a communications network, by defining a random secret key at a first one of the group of nodes. The random secret key is sent from the first one of the group nodes to remaining ones of the group of nodes. A random number is generated at a second one of the group of nodes. A one-way hash of the random number and the random secret key is performed at the second one of the group of nodes to generate a working key. A message is encrypted at the second one of the group of nodes, using the working key. The encrypted message and the random number are sent from the second one of the group of nodes to remaining ones of the group of nodes. The encrypted message and the random number are received at the remaining ones of the group of nodes. Each of the remaining ones of the group of nodes performs a one-way hash of the random number and the random secret key, to regenerate the working key. The message is then decrypted using the regenerated working key. The secret key may be defined at any one of the group of nodes rather than a predefined, centralized key distribution center. Moreover, the random number may be generated at any one of the group of nodes that desires to communicate

an encrypted message to remaining ones of the group of nodes. Decentralized group key management is thereby provided.

However, there are differences between Peyravian and the current application. In general, Peyravian describes a system and method for sending secure messages from a group of nodes (which are connected in a network) by defining a secret key at any one of the nodes. A message is encrypted at any one of the nodes with a session key that is generated from the secret key. The encrypted message is sent to the remaining nodes of the group. (See Peyravian, col. 2, lines 41-51.) The Peyravian system does not use a centralized group key distribution center; rather, only the member nodes of the group may generate and distribute group keys. This allows the nodes in the group to send secure messages without having to send the session key to each individual node. (See Peyravian, col. 2, lines 54-63.) Significantly, however, Peyravian does not describe or suggest that a new group session key is determined by replicating a branch of a binary tree. On the contrary in col. 2, line 67 to col. 3, line 17, Peyravian expressly describes that a working key, which a particular node may use to decrypt messages received from other nodes, is generated by computing a one-way hash from a random secret key (which is received from a first node) and from a random number (which is received from a second node). There is absolutely nothing in Peyravian that describes or suggests determining a session key by replicating a branch of a binary tree. In col. 6, lines 43-67, Peyravian describes that a secret key K may be distributed to the member nodes of a group in several different ways. In one way, the node sending the secret key K may encrypt K under the public key of the receiving node and sign this encrypted value using the sending node's private signature-generating key. (See Peyravian, col. 6, lines 44-47.) In another way, the node sending the secret key K may use a conventional

Diffie-Hellman key establishment protocol to first establish a common shared key with the receiving node and then encrypt K with this shared secret key. (See Peyravian, col. 6, lines 48-52.) Significantly, however, Peyravian does not describe that any form of replication may be used to distribute a new session key when a new node joins the group of nodes. In contrast, Claim 1 comprises the feature of determining a new group session key by replicating a branch of the second binary tree when an additional member node joins the multicast group. Neither the above passages nor any other passage from Peyravian describes or suggests that replication is used in determining a new session key. There is nothing in Peyravian that describes or suggests a directory service and a plurality of domains of the directory service. Independent claims 59, 81 and 102 include features similar to the features of claim 1, discussed above. Thus claims 59, 81 and 102 are patentable for at least the reasons given with respect to claim 1.

Any claims not directly addressed are allowed on the virtue of their dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131